IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	)	
	)	
Wheeler, et al.	)	
	)	Art Unit: **2137**
Application No. **09/923,213**	)	
	)	Examiner:
Filed: August 6, 2001	)	Kevin R. Schubert
	)	
For: **MANUFACTURING UNIQUE DEVICES THAT GENERATE DIGITAL SIGNATURES**	)	Confirmation No.: **8986**

CERTIFICATE UNDER 37 CFR 1.8: I hereby certify that this correspondence is being □ deposited with the United States Postal Service as First Class mail in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450, or □ filed via facsimile at 571 272 8300 or ☒ filed via EFS-Web, on August 21, 2006.

By: _____
John R. Harris

Mail Stop: Appeal Brief -- Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPELLANT'S APPEAL BRIEF PURSUANT TO 37 C.F.R. §41.31

Sir:

Pursuant to the provisions of 37 C.F.R. §41.31(a), Appellants hereby appeal the pending rejection of claims 1–5 and 21–31, which have been rejected in the February 21, 2006 Office Action.

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

The real party in interest in this appeal is First Data Corporation of Greenwood Village, Colorado, the assignee of record.

II. RELATED APPEALS AND INTERFERENCES

There are no other known appeals or interferences related to this appeal.

III. STATUS OF CLAIMS

Claims 1–5 and 21–31 are pending in this application and were rejected by the Patent Examiner in a Final Office Action dated February 21, 2006. The Appellants submitted a Pre-Appeal Brief Request for Review on May 22, 2006. The Panel responded on June 13, 2006 to the Appellants' Pre-Appeal Brief Request for Review maintaining the rejections of claims 1–5 and 21–31 and stating that the application remains under appeal. Claim 1–5 and 21–31 are the subject of this appeal.

IV. STATUS OF AMENDMENTS

Appellants submitted amendments pursuant to 37 C.F.R. §1.116 on August 18, 2006 addressing the Examiner's rejection of claims 1 and 24–29 under 35 U.S.C. §112, second paragraph. A true and correct copy of that amendment is attached hereto as Appendix A. Appellants respectfully request the entry of the amendment under 37 C.F.R. §1.116

V. SUMMARY OF CLAIMED SUBJECT MATTER

The following is a concise explanation of the invention set forth in the sole independent claim at issue, claim 1. The invention of the present application, as recited in claims 1–5 and 21–31, generally relates to a method of manufacturing devices that generate digital signatures so that each device may be reliably and uniquely identified. (*See* Application No. 09/923,213, page 6, lines 5–24) The method of the present invention generally involves creating a public-private key pair within each device during manufacture (*Id.*, page 7, lines 9–10), exporting the public key from the device to third parties (*Id.*, page 7, lines, 10–11) retaining the private key within the device (*Id.*, page 7, lines 14–15), and securely linking the exported public key with other information within a database within the secure environment of the manufacture of the device (*Id.*, page 7, lines 10–14 and 15–19). Each device manufactured according to the present invention is securely bound with its respective public key. (*Id.*, page 7, lines 12–25)

Independent claim 1 is directed to a method of manufacturing devices that generate digital signatures as described above comprising the specific steps of (a) creating a public-private key pair within a secure environment, the private key for utilization in generating a digital signature for an electronic message, the public key exportable for use by third parties in connection with authenticating the electronic message; (b) storing the private key within the device against the possibility of divulgement thereof by the device; and (c) securely linking the public key with other information by storing the public key and the other information in a database within the secure environment. (*Id.*, page 7, lines 8–25) The "other information" of claim 1 includes the information needed to assist the recipient of an

electronic message to reliably and uniquely identify the device. (*Id.*, page 7, lines 26–36 – page 8, lines 1–2)

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

In a final rejection mailed February 21, 2006, the Examiner rejected claims 1–5 and 21–31, and those claims are the subject of this appeal.

Claims 1–5 and 21–31 stand rejected on grounds of nonstatutory double patenting over U.S. Patent Nos. 6,915,430 and 6,892,302 and copending U.S. Patent Application Nos. 10/248,626 and 10/248,629. The issue in the present appeal is whether claims 1–5 and 21–31 are met by each of the four cited references.

Claims 1 and 24–29 stand rejected under 35 U.S.C. §112, second paragraph. Appellants addressed these rejections in the amendment filed on August 18, 2006 under 37 C.F.R. §1.116. Therefore, Appellants believe these issues are now moot.

Claims 1, 4–5, 21, and 25 stand rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,422,953 issued to *Fischer*. The issue in the present appeal is whether claims 1, 4–5, 21, and 25 are anticipated by *Fischer*.

Claims 2–3 stand rejected under 35 U.S.C. §103(a) as being unpatentable over *Fischer* in view of U.S. Patent No. 6,230,269 issued to *Spies et al.* The issue on this appeal is whether claims 2–3 are unpatentable under 35 U.S.C. §103(a) over *Fischer* in view of *Spies et al.*

Claims 22–24 and 27–28 stand rejected under 35 U.S.C. §103(a) as being unpatentable over *Fischer* in view of U.S. Patent No. 6,233,577 issued to *Ramasubramani et al.* This issue on this appeal is whether claims 22–24 and 27–28 are unpatentable under 35 U.S.C. §103(a) over *Fischer* in view of *Ramasubramani et al.*

Claim 26 stands rejected under 35 U.S.C. §103(a) as being unpatentable over *Fischer* in view of *Schneier* (Bruce Schneier, Applied Cryptography 185–187 (John Wiley & Sons 1996)). The issue on this appeal is whether claim 26 is unpatentable under 35 U.S.C. §103(a) over *Fischer* in view of *Schneier*.

Claims 29–31 stand rejected under 35 U.S.C. §103(a) as being unpatentable over *Fischer* in view of *Menezes* (Alfred J. Menezes, Handbook of Applied Cryptography 25–32,

546–548, 572–577 (CRC Press 1997)). The issue on this appeal is whether claims 29–31 are unpatentable over *Fischer* in view of *Menezes*.

For the reasons that follow, it is respectfully submitted that the present claims are patentable over the prior art references cited by the Examiner.

VII. ARGUMENT

A. THE EXAMINER'S REJECTION BASED ON NONSTATUTORY DOUBLE PATENTING HAS BEEN APPLIED IN AN OVERLY BROAD MANNER

Appellants respectfully traverse the Patent Examiner's rejection of claims 1–5 and 21–31 under the judicially created doctrine of obviousness–type double patenting over claim 17 of U.S. Patent No. 6,915,430, over claim 18 of U.S. Patent No. 6,892,302, over claim 28 of copending U.S. Patent Application No. 10/248,626, and over claim 35 of copending U.S. Patent Application No. 10/248,629.

In Appellants' response to the Examiner's September 7, 2005 Office Action filed on February 7, 2006, Appellants agreed to submit a terminal disclaimer of the present application directed to U.S. Patent No. 6,915,430, U.S. Patent No. 6,892,302, and U.S. Patent Application No. 10/248,626 because of the similarity in subject matter claimed in each of these references. Appellants remain willing to submit a terminal disclaimer directed to these references, and request the opportunity to submit the terminal disclaimer upon indication of allowable subject matter. However, Appellants do not agree with and hereby continue to traverse the Patent Examiner's assertion that the claims of the present application are not patentably distinct from the claims of U.S. Patent Application No. 10/248,629 (now U.S. Patent No. 6,959,381) ("the '381 Patent").

Specifically, the '381 Patent, which is entitled "Central Key Authority Database for User Accounts in ABDS System," is clearly directed to a three party system having a Central Key Authority (CKA), account holders, and account authorities, and includes the methods of managing a database by a central key authority for a plurality of account holders. In particular, the '381 Patent is directed to a method of maintaining a CKA computer database by a Central Key Authority on behalf of a plurality of users having accounts linked with one

or more public keys of the users ("PuK-linked accounts"). The one or more PuK-linked accounts in this patent are maintained by one or more respective third parties. The method includes various steps, including storing in the CKA computer database a public key of a public-private key pair, the public key associated with a user device of a respective user, the user device configured to generate digital signatures using a private key of the public-private key pair, the private key maintained securely within the user device, as well as associating in the CKA computer database a security profile of the user device with the public key.

However, and significantly, the '381 Patent claims (e.g. see claim 1) also recite the step of associating in the CKA computer database one or more third-party account identifiers with the public key, each account identifier associated with a respective PuK-linked account of the respective user maintained by one of the respective third parties. Further, there is the step of associating a unique CKA account identifier with each public key stored in the CKA computer database. Further still, the '381 Patent claim recites updating PuK-linked accounts of the respective user with a new public key of the respective user. Even more detailed steps are recited in the claim, relating to receiving a request "Electronic Communication," and authenticating a message, and sending a message to various third parties, etc.

The particular method claimed in the '381 Patent, it is submitted, is patentably distinct, and not obvious in view of the claimed subject matter in the present application. Although the present application and the '381 Patent contemplate devices used to originate digital signatures, the subject matter of the present application versus the three party system of the '381 Patent are distinct and non-obvious over each other. Accordingly, it is not believed that that the policies of the obviousness-type double patenting rejection are applicable in this situation because of the many different aspects and steps recited in the '381 Patent, and would not create any unjustified or improper time-wise extension of the right to exclude granted by a patent. It is thus requested that the requirement for a Terminal Disclaimer with respect to the '381 Patent be reconsidered and withdrawn.

For this reason, once the pending claims of the present application have been otherwise deemed allowable over the cited references, Appellants are willing to submit a

terminal disclaimer for the present application in relation to U.S. Patent No. 6,915,430, U.S. Patent No. 6,892,302, and U.S. Patent Application No. 10/248,626. However, Appellants object to and do not believe that a terminal disclaimer is necessary or proper since the claims of the present invention are patentably distinct from the claims of U.S. Patent Application No. 10/248,629 (now U.S. Patent No. 6,959,381).

B. CLAIMS 1 AND 24–29, AS AMENDED, COMPLY WITH THE REQUIREMENTS OF 35 U.S.C. §112

In the Office Action dated February 21, 2006, the Examiner rejected claims 1 and 24–29 as being allegedly vague or indefinite under 35 U.S.C. §112. Appellants addressed these rejections in the amendment filed on August 18, 2006 under 37 C.F.R. §1.116 and amended the claims to remove those issues from this appeal. Accordingly, Appellants assert that claims 1 and 24–29, as amended, comply with 35 U.S.C. §112. As such, Appellants respectfully request the entry of the amendment under 37 C.F.R. §1.116 and withdrawal of these rejections.

C. THE PATENT EXAMINER IMPROPERLY REJECTED CLAIMS 1, 4–5, 21, AND 25 UNDER 35 U.S.C. §102(b) AS BEING ANTICIPATED BY U.S. PATENT NO. 5,422,953 ISSUED TO *FISCHER*

By way of the Office Action dated February 21, 2006, the Examiner rejected claims 1, 4–5, 21 and 25 under 35 U.S.C. §102(b) as being allegedly unpatentable over U.S. Patent No. 5,422,953 issued to *Fischer*. This rejection is respectfully traversed.

For a claim to be anticipated under 35 U.S.C. §102(b), all elements of Appellants' claimed invention must be disclosed within a single reference. "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Appellants assert that *Fischer* fails to describe each and every element of Appellants' inventions as expressed in the claims.

In general, *Fischer* describes a personal date/time notary device (e.g., Smart Card, Smart Disk, token, etc.) that is a secure device that digitally signs messages that include a date/time stamp. The private key is maintained within the device, which defines its own

secure, tamper-resistant environment, to deter unauthorized access to, taking of, or tampering with the private key and the internal date/time clock. Trust and authenticity of the device, the private key, and the internal date/time clock is determined and reliably identified solely based upon one or more digital certificates that accompany a digital signature and time/date stamp originated by such devices. See FIG. 3, components 61, 62, of *Fischer* and related discussion. Such digital certificates include a single manufacturer's certificate 61 attesting to the fact that the device is trusted (see col. 5, ll. 60-62) and that the time-date stamp is accurate. A user's digital certificate 62 issued by a certification authority attests to the fact that the person possessing the device is the authorized user of the device. The use of digital certificates in *Fischer* to authenticate a digitally signed message describes a certificate authority digital signature (CADS) system.

As stated above, Appellants' invention is generally directed to a method of manufacturing devices, within a secure environment, that generate digital signatures so that each device may be reliably and uniquely identified without the need of digital certificates. According to Appellants' invention as embodied in independent claim 1 and its associated dependent claims, the method of the present invention involves creating a public-private key pair within each device during manufacture. The private key is retained within the device, while the public key is securely linked with other information, such as security features and a manufacturing history of each device, by storing the public key and the other information in a database within the secure environment of the manufacture of the device. Claim 5 of the present application teaches identification of a particular manufactured device which generates a digital signature by authenticating an electronic message using one of a plurality of public keys in the database within the secure environment. The authentication of an electronic message without the use of digital certificates as in the present application describes an account authority digital signature (AADS) system.

1. Distinctions Between *Fischer* and Appellants' Invention as Set Forth in Claim 1

The device manufactured according to Appellants' described method differs from the device described in *Fischer*. Appellants concede that *Fischer* contemplates that a

manufacturer/certifier could issue a combined digital certificate attesting that the device is authentic and accurate and attesting to the user's identity if the user is able to present himself to the manufacturer to obtain such a certification. However, *Fischer* teaches away from the presently claimed invention. Most notably, *Fischer* does not teach storing the public key and the other information in a database within the secure environment of the manufacture of the device. No such manufacturing environment is shown in *Fischer*.

In the Office Action, the Examiner indicated that *Fischer* provides for creating a public-private key pair "within a secured [sic] environment" and "securely linking the public key with other information within the secure environment." Appellants have diligently studied *Fischer* and are unable to locate any relevant information on which the Examiner could reasonably rely upon in making such a rejection. Thus, Appellants assert that the Examiner's rejection under 35 U.S.C. §102(b) is improper and should be withdrawn. *Fischer* does not describe a database for storing the public key in association with the other information. Claim 1 clearly points out that the step of securely linking the public key with other information is by storing the public key and the other information in a database within the secure environment. As evident in the dependent claim structure, the "other information" stored in the database in association with the public key can be of various types, for example, security-related information such as security features and manufacturing history of the device (claim 4), the identity of a plurality of third-parties with which an account is maintained (claim 22), user-specific information (claim 25), etc.

Furthermore, the "secure environment" in *Fischer*, following the Examiner's reasoning, can only be the device itself. There is clearly no database in the *Fischer* device itself for storing the public key in association with other information. Appellants point out that the claimed method is for manufacturing devices that generate digital signatures such that each device may be reliably and uniquely identified, the devices being manufactured within a secure environment. Such a secure "manufacturing" environment cannot be a "secure environment" defined by a device itself, as suggested by the Examiner's reliance on *Fischer*, because a device itself cannot define a manufacturing environment in which it itself is created. This assertion simply makes no sense.

Thus, the Examiner's reliance upon *Fischer* to show a device having a "secure environment" for manufacturing is not applicable. There is no storage in *Fischer* of other information in association with the public key in a database in the secure environment. For this reason alone, claim 1 is not anticipated, as *Fischer* fails to describe, teach or suggest any storage of a public key in association with other information in a database in a secure environment associated with manufacturing of the device.

Moreover, Appellants' invention describes a method of manufacturing devices within a secure environment that generate digital signatures so that each device may be reliably and uniquely identified. Appellants' invention describes an AADS system in which the devices manufactured are identified by using the public key and the other information stored in a database within the secure environment. Contrary to Appellants' invention, *Fischer* describes a CADS system in which an entity associated with the private key of a digital signature is identified by using digital certificates. *Fischer* does not describe a method of manufacturing devices, within a secure environment, that generate digital signatures such that each device may be reliably and uniquely identified without the need of a digital certificate. The present application and *Fischer* describe two totally different conceptual authentication models.

The Examiner cites an excerpt from *Fischer* on page 11, line 9 of the Office Action, which states "certificates may be [*sic*, are] stored externally to the device (e.g., in storage associated with a computer driving the notary device) or internally . . .," to support the assertion that *Fischer* describes storing the public key and the other information in a database. Appellants cannot understand how the Examiner can reasonably rely on this passage as anticipatory and therefore respectfully submit that the Board should overrule the Examiner's assertion. As previously stated, it is certificates that are stored in *Fischer*, not the public key and other information, and not in conjunction with manufacturing devices such that each device may be reliably and uniquely identified without the use of digital certificates.

2. Conclusion

As demonstrated above, the Examiner has failed to establish that *Fischer* anticipates each and every element of Appellants' claimed invention, especially claim 1. *Fischer* does not teach or suggest manufacturing a digital signature device within a "secure environment."

Fischer also does not teach or suggest a method for manufacturing devices that generate digital signatures such that each device may be reliably and uniquely identified, the devices being manufactured within a secure environment. Therefore, the claims that depend on claim 1, in particular claims 4–5, 21, and 25, are not anticipated by the *Fischer* reference. Appellants submit that pending claims 1, 4–5, 21, and 25 recite inventions that are novel over the art cited by the Examiner, as the art fails to teach or disclose the claimed aspects of manufacturing digital signature devices as claimed in the claims submitted herein. Accordingly, it is respectfully submitted that claims 1, 4–5, 21, and 25 are not anticipated by *Fischer*, and it is requested that the rejection be withdrawn.

D. THE PATENT EXAMINER IMPROPERLY REJECTED CLAIMS 2–3 UNDER 35 U.S.C. §103(a) AS BEING OBVIOUS OVER *FISCHER* IN VIEW OF U.S. PATENT NO. 6,230,269 ISSUED TO *SPIES*

In the Office Action dated February 21, 2006, the Examiner rejected claims 2–3 under 35 U.S.C. §103(a) as being allegedly obvious over *Fischer* in view of *Spies*. This rejection is respectfully traversed.

1. The Patent Examiner Failed to Make a Prima Facie Case of Obviousness to Support a Rejection of Claims 2–3 under 35 U.S.C. §103(a) over *Fischer* in View of *Spies*

"The Patent Examiner bears the initial burden of factually supporting any *prima facie* conclusion of obviousness." *See* MPEP §2142. To establish a *prima facie* case of obviousness pursuant to the MPEP, the Patent Examiner must meet three basic criteria. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference or combination of references must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on Appellants' disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991); MPEP §2142.

For the reasons articulated below, it is respectfully submitted that the Examiner failed to make a *prima facie* case to support a rejection of any claims under 35 U.S.C. §103(a) over *Fischer* in view of *Spies*.

a. There is no suggestion or motivation to modify the references or combine the *Fischer* and *Spies* references

Obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. *In re Fine*, 837 F.2d 1071, 5 U.S.P.Q.2d 1596 (Fed. Cir. 1988); *In re Jones*, 958 F.2d 347, 21 U.S.P.Q.2d 1941 (Fed. Cir. 1992).

Appellants submit that the Examiner has failed to identify any suggestion or motivation to modify the references or combine the teachings of *Fischer* and *Spies*. As such, the Examiner has failed to make a *prima facie* case of obviousness under 35 U.S.C. §103(a). Therefore, the rejection is improper and should be withdrawn.

In the Office Action dated February 21, 2006, the Examiner asserted that, as per claim 2, Appellants describe the method of claim 1, which is met by *Fischer*, with the following limitation which is met by *Spies*: Wherein each private-public key pair is created within each device based on a random number produced by a random number generator disposed within each device (*Spies*, claim 16). In essence, the Examiner combined the teachings of *Fischer* with the teachings of *Spies* to support a rejection under 35 U.S.C. §103(a). Specifically, the Examiner relied upon claim 16 of *Spies* for disclosure of a random number generator.

In general, *Spies* teaches distributed cryptographic authentication systems implemented on distributed computer networks having one or more servers interconnected to one or more clients. (*Spies* Col. 1, ll. 5–10). Claim 16 of *Spies* covers a method for operating an authentication system on a distributed network having a client and a server comprising the step of generating a public-private key pair from a random number generator. *Spies* does not teach or suggest creating a public-private key pair within a device that generates digital signatures. Likewise, *Spies* does not teach or suggest a method of

manufacturing the devices in a secure environment. Rather, *Spies* describes the use of a random number generator itself for creating a public-private key pair.

Unlike *Spies*, claim 2 of the present application is not claiming the use of a random number generator by itself for use in connection with the claimed method of manufacturing devices that generate digital signatures. Rather, the public-private key pair of the present application is created within the device and is based on a random number produced by a random number generator. The notion of the random number generator of *Spies* does not meet claim 2 of Appellants' application as whole. The creation of the public-private key pair within the device based on a random number produced by a random number generator as well as the method of manufacturing steps of claim 1 are not disclosed, taught, or suggested as a whole by *Spies*. Furthermore, as discussed in detail above, *Fischer* does not describe all the limitations of claim 1 as asserted by the Examiner on page 6 of the February 21, 2006 Office Action. Neither the *Fischer* nor the *Spies* reference identifies the devices manufactured pursuant to the method of claim 2 of Appellants' application. Moreover, *Spies* does not describe the elements of Appellants' invention that are missing from *Fischer*, namely that *Fischer* describes a certificate authority digital signature system rather than an account authority digital signature system.

In the February 21, 2006 Office Action, the Examiner asserted that, as per claim 3, Appellants describe the method of claim 1, which is met by *Fischer*, with the following limitation which is met by *Spies*: Wherein each digital signature generated by each device is a random number (*Fischer*: Col. 4, ll. 2–7). Contrary to the Examiner's assertion, *neither Fischer* nor *Spies* show that the digital signature itself is a random number. Rather, these references show generation of a digital signature using a random number generator. Neither *Fischer* nor *Spies* teach, suggest, or disclose a digital signature generated by a device that is manufactured in a secure environment wherein the digital signature is a random number.

Given that there is no motivation to modify the teachings of *Fischer* with the teachings of *Spies*, the Examiner has failed to make a *prima facie* case of obviousness under 35 U.S.C. §103(a) with respect to the combination of *Fischer* and *Spies*. Appellants submit that

the Examiner is relying on an unreasonable interpretation and reliance on these references. Therefore, the rejection under 35 U.S.C. §103(a) is improper and should be withdrawn.

Appellants would also like to point out that claims 2–3 depend on claim 1. In other words, claims 2–3 further limitations than what is claimed in claim 1. Under the doctrine of *In re Fine*, 837 F.2d 1071, 5 U.S.P.Q.2d 1596 (Fed. Cir. 1988), if an independent claim is nonobvious under 35 U.S.C. §103(a), then any claim depending there from is nonobvious. Accordingly, since claim 1 is nonobvious, it follows that claims 2–3 are also nonobvious.

b. There is no reasonable expectation of success in combining the *Fischer* and *Spies* references

Appellants submit that the Examiner has failed to identify a reasonable expectation of success in combining the teachings of *Fischer* and *Spies*. As such, the Examiner has not established a *prima facie* case of obviousness under 35 U.S.C. §103(a). Therefore, the rejection is improper and should be withdrawn.

Appellants respectfully submit that there is no reasonable expectation of success in combining the reference teachings. The prior art can be modified or combined to reject claims as *prima facie* obvious as long as there is a reasonable expectation of success. *In re Merck & Co., Inc.*, 800 F.2d 1091, 231 U.S.P.Q. 375 (Fed. Cir. 1986). Obviousness does not require absolute predictability; however, at least some degree of predictability is required. Evidence showing there was no reasonable expectation of success may support a conclusion of nonobviousness. *In re Rinehart*, 531 F.2d 1048, 189 U.S.P.Q. 143 (CCPA 1976). In this instance, Appellants submit that there is no reasonable expectation of success in combining the teachings of *Fischer* and *Spies* to support a rejection under 35 U.S.C. §103(a).

As discussed in detail above, there is no motivation to combine the cited references. Neither the *Fischer* nor the *Spies* reference identifies the devices manufactured pursuant to the method of claims 2–3 of Appellants' application. Moreover, *Spies* does not describe the elements of Appellants' invention that are missing from *Fischer*, namely that *Fischer* describes a certificate authority digital signature system rather than an account authority digital signature system. As such, there is no expectation that combining the references would result in a successful combination. Furthermore, there is no expectation that combining the

references would result in Appellants' claimed inventions, as will be discussed in greater detail below.

c. The combination of the *Fischer* and *Spies* references does not teach or suggest all the elements of Appellants' claimed invention

To establish a *prima facie* case of obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). "All the words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970). Furthermore, if an independent claim is nonobvious under 35 U.S.C. §103, then any claim depending there from is nonobvious. *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988). Appellants assert that the combination of *Fischer* and *Spies* fails to teach or suggest all the elements of Appellants' claimed invention. Therefore, the Examiner's arbitrary combination of these references is insufficient to support a rejection under 35 U.S.C. §103(a).

As explained above, Appellants' inventions are generally directed to methods of manufacturing devices in a secure environment that generate digital signatures such that each device may be reliably and uniquely identified. The method claimed in claims 2–3 relate to creating a public-private key pair within the secure environment, storing the private key within the device, and securely linking the public key with other information by storing the public key and the other information in a database within the secure environment. Claim 2 of the present application further qualifies claim 1 in that the public-private key pair is created using a random number produced by a random number generator within each device. Claim 3 recites that the digital signature generated is a random number.

In general, neither *Fischer* nor *Spies* teach or suggest the method of manufacturing devices that generate digital signatures as recited in claims 2–3 of the present application. Specifically, neither *Fischer* nor *Spies* teach or suggest manufacturing a digital signature device within a "secure environment." The references also do not teach or suggest a method for manufacturing devices that generate digital signatures such that each device may be reliably and uniquely identified, the devices being manufactured within a secure environment.

Given that *Fischer* and *Spies* singularly or in combination do not teach or suggest all the elements of any of Appellants' claimed inventions, it is respectfully submitted that the Examiner has failed to establish a *prima facie* case of obviousness with respect to any of claims 2–3. Thus, the combination of *Fischer* and *Spies* is insufficient to support a rejection under 35 U.S.C. §103(a).

d. Conclusion

It is respectfully submitted that the Examiner has failed to make a *prima facie* case of obviousness. First, there is no motivation to combine the references. Second, there is no reasonable expectation of success in combining the references. And third, the combination of *Fischer* and *Spies* fails to teach and enable every element of Appellants' claimed inventions as set forth in claims 2–3. Furthermore, under the doctrine of *In re Fine*, claims 2–3 should be allowable since claim 1 is nonobvious under 35 U.S.C. §103(a). Therefore, the rejection under §103(a) with respect to the combination of *Fischer* and *Spies* is improper and should be withdrawn.

2. Appellants' Invention is Not Obvious over the Combination of *Fischer* and *Spies* Under the *Graham v. John Deere Factors*

In *Graham v. John Deere*, 383 U.S. 1, 148 U.S.P.Q. 459 (1966), the Supreme Court set forth four factual inquiries to be made when making an obviousness determination. First, the scope and content of the prior art is determined. Next, the differences between the prior art and the claims at issue is ascertained. Then, the level of ordinary skill in the art is resolved. Secondary considerations of nonobviousness may also be evaluated. Finally, a determination of obviousness is made. MPEP §2141.

For the reasons articulated below, it is respectfully submitted that Appellants' claimed inventions as recited in claims 2–3 are not obvious over *Fischer* in view of *Spies* under the principles of *Graham*.

a. Scope and content of the prior art

As stated above, *Fischer* describes a personal date/time notary device (e.g., Smart Card, Smart Disk, token, etc.) that is a secure device that digitally signs messages that include a date/time stamp, and *Spies* teaches distributed cryptographic authentication systems

implemented on distributed computer networks having one or more servers interconnected to one or more clients.

Neither *Fischer* nor *Spies* is directed to a method of manufacturing devices in a secure environment that generate digital signatures such that each device may be reliably and uniquely identified. Neither *Fischer* nor *Spies* is directed to creating the public-private key pair within the secure environment. Neither *Fischer* nor *Spies* is directed to storing the private key within the device and securely linking the public key with other information by storing the public key and the other information in a database within a secure environment. Neither *Fischer* nor *Spies* is directed to creating the public-private key pair based on a random number produced by a random number generator disposed in each device. And neither *Fischer* nor *Spies* is directed to devices that generate digital signatures that are random numbers.

b. Differences between the prior art and the claimed invention

Appellants' inventions, as recited in claims 2–3, are directed to methods of manufacturing devices within a secure environment that generate digital signatures such that each device may be reliably and uniquely identified. A public-private key pair is created within the secure environment. The private key, which is stored in the device, is utilized in generating the digital signature for an electronic message. The public key is exportable for use by third parties for authenticating the electronic message and securely linked with other information by storing the public key and the other information in a database within the secure environment. The "other information" includes the information needed to assist the recipient of an electronic message to reliably and uniquely identify the device. The invention of claim 2 of the present application further qualifies the invention of claim 1 by reciting that the public-private key pair is created within each device based on a random number produced by a random number generator disposed within the device. The invention of claim 3 of the present application recites that the digital signature generated by the device is a random number.

In general, neither of the references, alone or in combination, teach or suggest the method of manufacturing devices within a secure environment that generate digital signatures as set forth in claims 2–3. In particular, with respect to claim 1 from which claims

2–3 depend, the combination of *Fischer* and *Spies* fails to teach or suggest a method for manufacturing devices that generate digital signatures. The combination of the references fails to teach or suggest manufacturing the devices in a secure environment. The combination of the references fails to teach or suggest that each device may be reliably and uniquely identified by any means other than a certificate. And finally, the combination of the references fails to teach or suggest a database within a secure environment in which the public key and other information is stored.

With respect to claim 2, which builds upon the elements presented in claim 1, the combination of *Fischer* and *Spies* fails to further teach or suggest, *inter alia*, creating the public-private key pair within each device based on a random number produced by a random number generator disposed within each device.

With respect to claim 3 which builds upon the elements presented in claims 1 and 2, the combination of *Fischer* and *Spies* fails to teach or suggest, *inter alia*, that the digital signature generated by each device is a random number.

c. Level of ordinary skill in the art

Appellants respectfully submit that the level or ordinary skill in the art is one who is skilled in electronic communications and digital signatures.

d. Obviousness analysis

Appellants respectfully submit that the claimed inventions as summarized above would not be obvious to one skilled in electronic communications and digital signatures in view of *Fischer* and *Spies*. As stated above, neither *Fischer* nor *Spies* teach or suggest the method of manufacturing devices that generate digital signatures as recited in claims 2–3 of the present application. Specifically, neither *Fischer* nor *Spies* teach or suggest manufacturing a digital signature device within a "secure environment." The references also do not teach or suggest a method for manufacturing devices that generate digital signatures such that each device may be reliably and uniquely identified, the devices being manufactured within a secure environment. Since these (and other) aspects of Appellants' inventions are not taught or suggested by any of the references, it is not likely that one of skill in the art would find it obvious to manufacture devices that generate digital signatures according to claims 2–3 of

Appellants' claimed inventions. The omitted elements are not mere variations of the prior art, nor are they so well known that no reference is needed to supply the missing element. Thus, Appellants' claimed invention would not be obvious to one of ordinary skill in the art over *Fischer* and *Spies*.

e. Conclusion

Appellants respectfully submit that using the *John Deere* factual inquires, the differences between the prior art and the inventions as claimed in claims 2–3 of the present application would not be obvious to one of ordinary skill in the art. Accordingly, Appellants respectfully request withdrawal of the rejection of claims 2–3 under 35 U.S.C. §103(a).

E. THE PATENT EXAMINER IMPROPERLY REJECTED CLAIMS 22–24 AND 27–28 UNDER 35 U.S.C. §103(a) AS BEING OBVIOUS OVER *FISCHER* IN VIEW OF U.S. PATENT NO. 6,233,577 ISSUED TO *RAMASUBRAMANI*

In the Office Action dated February 21, 2006, the Examiner rejected claims 22–24 and 27–28 under 35 U.S.C. §103(a) as being allegedly obvious over *Fischer* in view of *Ramasubramani*. This rejection is respectfully traversed.

1. The Patent Examiner Failed to Make a Prima Facie Case of Obviousness to Support a Rejection of Claims 22–24 and 27–28 under 35 U.S.C. §103(a) over *Fischer* in View of *RAMASUBRAMANI*

For the reasons articulated below, it is respectfully submitted that the Examiner failed to make a *prima facie* case to support a rejection of any claims under 35 U.S.C. §103(a) over *Fischer* in view of *Ramasubramani*.

a. There is no suggestion or motivation to modify the references or combine the *Fischer* and *Ramasubramani* references

Appellants submit that the Examiner has failed to identify any suggestion or motivation to modify the references or combine the teachings of *Fischer* and *Ramasubramani*. As such, the Examiner has failed to make a *prima facie* case of obviousness under 35 U.S.C. §103(a). Therefore, the rejection is improper and should be withdrawn.

In the Office Action dated February 21, 2006, the Examiner asserted that, as per claim 22, Appellants' application describes the method of claim 1, which is met by *Fischer*,

with the following limitation which is met by *Ramasubramani*: Wherein the PuK-linked information (the public key and the other information) stored in the database includes the identity of a plurality of third-parties with which an account is maintained, the accounts being identified by one of a plurality of third-party account identifiers (*Ramasubramani*: Fig. 4B). The Examiner combined the teachings of *Fischer* with the teachings of *Ramasubramani* to support a rejection under 35 U.S.C. §103(a). The Examiner indicated that *Ramasubramani* discloses the idea that certificates are stored and maintained for a plurality of third parties in a centralized database, the accounts being identified by one of a plurality of third party account identifiers. It is important to note that *Ramasubramani* relates to digital certificates, which involves a different conceptual/authentication model than the present application, which involves authentication of digital signatures without the use of digital certificates.

In the February 21, 2006 Office Action, the Examiner also asserted that, as per claims 23–24 and 27–28, Appellants' invention describes the method of claim 1, which is met by *Fischer*, with the following limitation which is met by *Ramasubramani*: Wherein the PuK-linked account information (the public key and the other information) of the users is indexed in the database by unique account identifiers such that the PuK-linked account information (the public key and other information) for a user is retrievable from the database based on the account identifier (*Ramasubramani*: Fig. 4B).

In general, *Ramasubramani* teaches data security between server computers and client computers in data networks, and more particularly relates to systems for managing, in a proxy server computer, digital certificates for two-way interactive communication devices over the data networks. (Col. 1, ll. 28-32) Figure 4B of *Ramasubramani* demonstrates an example in which a user of a mobile device requests certificates from a user-specified Certification Authority. (Col. 2, ll. 58-60) *Ramasubramani* describes enclosing one or more digital certificates with every signed message. (Col. 4, lines 29-30) ("The most secure use of authentication involves enclosing one or more certificates with every signed message.").

The certificate enclosed with every message in *Ramasubramani* is used to authenticate a digitally signed message from a consumer using the public key of the certificate authority when the certificate is included with the digitally signed message. (Col. 4, lines 30-33) ("The

receiver of the message would verify the certificate using the certifying authority's public key and, now confident of the public key of the sender, verify the message's signature.") The use of digital certificates, as described by *Ramasubramani*, is known in the art, and is a factually and technically different model for authentication using public key-private key encryption.

Unlike *Ramasubramani*, which teaches a certificate authority digital signature (CADS) system, the present invention relates to an account authority digital signature (AADS) system. Furthermore, as discussed in detail above, *Fischer*, which also teaches a CADS system, does not describe all the limitations of claim 1 as asserted by the Examiner on page 7 of the February 21, 2006 Office Action. Neither *Fischer* nor *Ramasubramani* teach or describe systems or methods of manufacturing devices that generate digital signatures such that each device may be reliably and uniquely identified without the need of a digital certificate. Neither reference teaches anything about the manufacturing process for a digital signature device. One skilled in the art would not be motivated to take the CADS systems described by *Fischer* and *Spies* to arrive at the AADS system described in Appellants' present application, namely, a method of manufacturing devices in a secure environment that generate digital signatures such that each device may be reliably and uniquely identified without the use of digital certificates. Therefore, it is factually and legally improper for the Examiner to base a rejection of any claims of the present application on references that describe systems that are so conceptually different from, and teach away from, the present invention.

Given that there is no motivation to modify the teachings of *Fischer* with the teachings of *Ramasubramani*, the Examiner has failed to make a *prima facie* case of obviousness under 35 U.S.C. §103(a) with respect to the combination of *Fischer* and *Ramasubramani*. Therefore, the rejection under 35 U.S.C. §103(a) is improper and should be withdrawn.

Appellants would also like to point out that claims 22–24 and 27-28 depend on claim 1. In other words, these claims add further limitations than what is claimed in claim 1. Under the doctrine of *In re Fine*, 837 F.2d 1071, 5 U.S.P.Q.2d 1596 (Fed. Cir. 1988), if an independent claim is nonobvious under 35 U.S.C. §103(a), then any claim depending there

from is nonobvious. Accordingly, since claim 1 is nonobvious, it follows that claims 22–24 and 27–28 are also nonobvious.

b. There is no reasonable expectation of success in combining the *Fischer* and *Ramasubramani* references

Appellants submit that the Examiner has failed to identify a reasonable expectation of success in combining the teachings of *Fischer* and *Ramasubramani*. As such, the Examiner has not established a *prima facie* case of obviousness under 35 U.S.C. §103(a). Therefore, the rejection is improper and should be withdrawn.

In this instance, Appellants submit that there is no reasonable expectation of success in combining the teachings of *Fischer* and *Ramasubramani* to support a rejection under 35 U.S.C. §103(a). As discussed in detail above, there is no motivation to combine the cited references because one skilled in the art would not combine two references that teach CADS systems to arrive at an AADS system, as described in the present application. Moreover, neither *Fischer* nor *Ramasubramani* describe, *inter alia*, identifying the devices without the use of digital certificates, or do the cited references describe securely linking the public key with other information by storing the public key and the other information in a database within the secure environment in which the device was manufactured. As such, there is no expectation that combining the references would result in a successful combination. Furthermore, there is no expectation that combining the references would result in Appellants' claimed inventions, as will be discussed in greater detail below.

c. The combination of the *Fischer* and *Ramasubramani* references does not teach or suggest all the elements of Appellants' claimed invention

Appellants assert that the combination of *Fischer* and *Ramasubramani* fails to teach or suggest all the elements of Appellants' claimed invention, and therefore, is insufficient to support a rejection under 35 U.S.C. §103(a).

As explained above, Appellants' inventions are generally directed to AADS systems and to methods of manufacturing devices in a secure environment that generate digital signatures such that each device may be reliably and uniquely identified. The method claimed in claims 22–24 and 27–28 comprises creating a public-private key pair within the

secure environment, storing the private key within the device, and securely linking the public key with other information by storing the public key and the other information in a database within the secure environment. The devices manufactured according to the present application may be reliably and uniquely identified without the need of a digital certificate, unlike the *Fischer* and *Ramasubramani* references.

In general, neither *Fischer* nor *Ramasubramani* teach or suggest the method of manufacturing devices that generate digital signatures as recited in claims 22–24 and 27–28 of the present application. Specifically, neither *Fischer* nor *Ramasubramani* teach or suggest manufacturing a digital signature device within a "secure environment." The references also do not teach or suggest a method for manufacturing devices in a secure environment that generate digital signatures such that each device may be reliably and uniquely identified without the need of a digital certificate.

Given that the combination *Fischer* and *Ramasubramani* clearly does not teach or suggest all elements of any of Appellants' claimed inventions, it is respectfully submitted that the Examiner has failed to establish a *prima facie* case of obviousness with respect to any of claims 22–24 and 27–28. Thus, the combination of *Fischer* and *Ramasubramani* is insufficient to support a rejection under 35 U.S.C. §103(a).

d. Conclusion

It is respectfully submitted that the Examiner has failed to make a *prima facie* case of obviousness. First, there is no motivation to combine the references. Second, there is no reasonable expectation of success in combining the references. And third, the combination of *Fischer* and *Ramasubramani* fails to teach and enable every element of Appellants' claimed inventions as set forth in claims 22–24 and 27–28. Furthermore, under the doctrine of *In re Fine*, claims 22–24 and 27–28 should be allowable since claim 1 is nonobvious under 35 U.S.C. §103(a). Therefore, the rejection under §103(a) with respect to the combination of *Fischer* and *Ramasubramani* is improper and should be withdrawn.

2. Appellants' Invention is Not Obvious over the Combination of *Fischer* and *Ramasubramani* Under the *Graham v. John Deere Factors*

For the reasons articulated below, it is respectfully submitted that Appellants' claimed inventions as recited in claims 22–24 and 27–28 are not obvious over *Fischer* in view of *Ramasubramani*.

a. Scope and content of the prior art

As stated above, *Fischer* and *Ramasubramani* describe CADS systems that use certificates via a certificate authority to authenticate digitally signed messages.

Neither *Fischer* nor *Ramasubramani* is directed to a method of manufacturing devices in a secure environment that generate digital signatures such that each device may be reliably and uniquely identified without the need of a digital certificate. Neither *Fischer* nor *Ramasubramani* is directed to creating the public-private key pair within the secure environment. Neither *Fischer* nor *Ramasubramani* is directed to storing the private key within the device and securely linking the public key with other information by storing the public key and the other information in a database within the secure environment.

b. Differences between the prior art and the claimed invention

Appellants' inventions, as recited in claims 22–24 and 27–28, are directed to methods of manufacturing devices within a secure environment that generate digital signatures such that each device may be reliably and uniquely identified without the need of digital certificates. A public-private key pair is created within the secure environment. The private key, which is stored in the device, is utilized in generating the digital signature for an electronic message. The public key is exportable for use by third parties for authenticating the electronic message and securely linked with other information by storing the public key and the other information in a database within the secure environment. The "other information" involves the information needed to assist the recipient of an electronic message to reliably and uniquely identify the device. There is no digital certificate in any of the claims at issue used to identify the device. The inventions described in *Fischer* and *Ramasubramani*

are conceptually different models as compared to the present application in that digital certificates are used.

In general, neither of the references, alone or in combination, teach or suggest the method of manufacturing devices within a secure environment that generate digital signatures as set forth in claims 22–24 and 27–28. In particular, with respect to claim 1 from which claims 22–24 and 27–28 depend, the combination of *Fischer* and *Ramasubramani* fails to teach or suggest a method for manufacturing devices that generate digital signatures. The combination of the references fails to teach or suggest manufacturing the devices in a secure environment. The combination of the references fails to teach or suggest that each device may be reliably and uniquely identified by any means other than a certificate. And finally, the combination of the references fails to teach or suggest a database within a secure environment in which the public key and other information is stored.

With respect to claim 22 which builds upon the elements presented in claim 1, the combination of *Fischer* and *Ramasubramani* fails to further teach or suggest, *inter alia*, that the public key and other information stored in the database within the secure environment includes the identity of a plurality of third-parties with which an account is maintained, the accounts being identified by one of a plurality of third-party account identifiers. No reference meets this limitation.

With respect to claim 23 which builds upon the elements presented in claims 1 and 22, the combination of *Fischer* and *Ramasubramani* fails to teach or suggest, *inter alia*, that the public key and the other information of the users is indexed in the database by unique account identifiers such that the public key and the other information for a user is retrievable from the database based on the account identifier. No reference meets this limitation.

With respect to claim 24 which builds upon the elements presented in claims 1 and 22–23, the combination of *Fischer* and *Ramasubramani* fails to teach or suggest, *inter alia*, that the public key is the unique account identifier. Once again, the Examiner has neglected to demonstrate how either of the cited references meets this limitation.

With respect to claim 27 which builds upon the elements presented in claim 1, the combination of *Fischer* and *Ramasubramani* fails to teach or suggest, *inter alia*, establishing an

account on behalf of a user of a device with a third-party by communicating the public key of the device and the other information linked with the public key from the database to the third-party. And once again, the Examiner has neglected to demonstrate how either of the cited references meets this limitation.

With respect to claim 28 which builds upon the elements presented in claim 1, the combination of *Fischer* and *Ramasubramani* fails to teach or suggest, *inter alia*, that the public key of the device and the other information linked with the public key is communicated to a third party upon the request of the third-party. Indeed, the Examiner has neglected to demonstrate how either of the cited references meets this limitation.

c. Level of ordinary skill in the art

Appellants respectfully submit that the level or ordinary skill in the art is one who is skilled in electronic communications and digital signatures.

d. Obviousness analysis

Appellants respectfully submit that the claimed inventions as summarized above would not be obvious to one skilled in electronic communications and digital signatures in view of *Fischer* and *Ramasubramani*. As stated above, neither *Fischer* nor *Ramasubramani* teach or suggest the method of manufacturing devices that generate digital signatures as recited in claims 22–24 and 27–28 of the present application. Specifically, neither *Fischer* nor *Ramasubramani* teach or suggest manufacturing a digital signature device within a "secure environment." The references also do not teach or suggest a method for manufacturing devices that generate digital signatures such that each device may be reliably and uniquely identified without the need of a digital certificate, the devices being manufactured within a secure environment. Because these (and other) aspects of Appellants' inventions are not taught or suggested by any of the references, it is not likely that one of skill in the art would find it obvious to manufacture devices that generate digital signatures according to claims 22–24 and 27–28 of Appellants' claimed inventions. The omitted elements are not mere variations of the prior art, nor are they so well known that no reference is needed to supply the missing element. Thus, Appellants' claimed invention would not be obvious to one of ordinary skill in the art over *Fischer* and *Ramasubramani*.

e. Conclusion

Appellants respectfully submit that using the *John Deere* factual inquires, the differences between the prior art and the inventions as claimed in claims 22–24 and 27–28 of the present application would not be obvious to one of ordinary skill in the art. According, Appellants respectfully request withdrawal of the rejection of claims 22–24 and 27–28 under 35 U.S.C. §103(a).

F. THE PATENT EXAMINER IMPROPERLY REJECTED CLAIM 26 UNDER 35 U.S.C. §103(a) AS BEING OBVIOUS OVER *FISCHER* IN VIEW OF *SCHNEIER*

In the Office Action dated February 21, 2006, the Examiner rejected claim 26 under 35 U.S.C. §103(a) as being allegedly obvious over *Fischer* in view of *Schneier* (Bruce Schneier, Applied Cryptography 185–187 (John Wiley & Sons 1996)). This rejection is respectfully traversed.

1. The Patent Examiner Failed to Make a Prima Facie Case of Obviousness to Support a Rejection of Claims 22–24 under 35 U.S.C. §103(a) over *Fischer* in View of *Schneier*

For the reasons articulated below, it is respectfully submitted that the Examiner failed to make a *prima facie* case to support a rejection of any claims under 35 U.S.C. §103(a) over *Fischer* in view of *Schneier*.

a. There is no suggestion or motivation to modify the references or combine the *Fischer* and *Schneier* references

Appellants submit that the Examiner has failed to identify any suggestion or motivation to modify the references or combine the teachings of *Fischer* and *Schneier*. As such, the Examiner has failed to make a *prima facie* case of obviousness under 35 U.S.C. §103(a). Therefore, the rejection is improper and should be withdrawn.

In the Office Action dated February 21, 2006, the Examiner asserted that, as per claim 26, because Appellants' invention depended on claim 1 which is met by *Fischer*, the following limitation which is met by *Schneier*: Wherein the user-specific information includes the name and address of the user (*Schneier*: page 186). The Examiner combined the teachings of *Fischer* with the teachings of *Schneier* to support a rejection under 35 U.S.C. §103(a). The

Examiner indicated that *Schneier* discloses the idea that a certificate may disclose the name and address of a user.

Like the *Fischer* and *Ramasubramani* references discussed in detail above, *Schneier* teaches a certificate authority system for authenticating the information about the user of a public key. *Schneier* also teaches that the certificate authority certifies that the public key indeed belongs to the correct user of the public key. As stated above, the use of digital certificates, as described by *Schneier*, is known in the art, and is a factually and technically different model for authentication using public key/private key encryption.

Unlike *Schneier*, which teaches a use of a certificate authority, the present invention describes an account authority digital signature (AADS) system. Furthermore, as discussed in detail above, *Fischer*, which teaches a CADS system, does not describe all the limitations of claim 1 as asserted by the Examiner on page 8 of the February 21, 2006 Office Action. Neither *Fischer* nor *Schneier* teaches or discloses systems or methods of manufacturing devices that generate digital signatures such that each device may be reliably and uniquely identified without the need of a digital certificate. Neither reference teaches anything about the manufacturing process for a digital signature device. Therefore, it is factually and legally improper for the Examiner to base a rejection of any claims of the present application on references that describe systems that are so conceptually different from, and teach away from, the present invention.

Given that there is no motivation to modify the teachings of *Fischer* with the teachings of *Schneier*, the Examiner has failed to make a *prima facie* case of obviousness under 35 U.S.C. §103(a) with respect to the combination of *Fischer* and *Schneier*. Therefore, the rejection under 35 U.S.C. §103(a) is improper and should be withdrawn.

Appellants would also like to point out that claim 26 depends on claim 25 which depends on claim 1. In other words, claim 26 adds further limitations to that which is claimed in claims 1 and 25. Under the doctrine of *In re Fine*, 837 F.2d 1071, 5 U.S.P.Q.2d 1596 (Fed. Cir. 1988), if an independent claim is nonobvious under 35 U.S.C. §103(a), then any claim depending there from is nonobvious. Accordingly, since claim 1 is nonobvious, it follows that claim 26 is also nonobvious.

b. There is no reasonable expectation of success in combining the *Fischer* and *Schneier* references

Appellants submit that the Examiner has failed to identify a reasonable expectation of success in combining the teachings of *Fischer* and *Schneier*. As such, the Examiner has not established a *prima facie* case of obviousness under 35 U.S.C. §103(a). Therefore, the rejection is improper and should be withdrawn.

In this instance, Appellants submit that there is no reasonable expectation of success in combining the teachings of *Fischer* and *Schneier* to support a rejection under 35 U.S.C. §103(a). As discussed in detail above, there is no motivation to combine the cited references because one skilled in the art would not combine two references that teach CADS systems to arrive at an AADS system, as described in the present application. Moreover, neither *Fischer* nor *Schneier* describe, *inter alia*, identifying the devices without the use of digital certificates, nor do the cited references describe manufacturing digital signature devices. As such, there is no expectation that combining the references would result in a successful combination. Furthermore, there is no expectation that combining the references would result in Appellants' claimed inventions, as will be discussed in greater detail below.

c. The combination of the *Fischer* and *Schneier* references does not teach or suggest all the elements of Appellants' claimed invention

Appellants assert that the combination of *Fischer* and *Schneier* fails to teach or suggest all the elements of Appellants' claimed invention, and therefore, is insufficient to support a rejection under 35 U.S.C. §103(a).

As explained above, Appellants' inventions are generally directed to methods of manufacturing devices in a secure environment that generate digital signatures such that each device may be reliably and uniquely identified without the need of a digital certificate. The method claimed in claim 26 recites creating a public-private key pair within the secure environment, storing the private key within the device, and securely linking the public key with other information by storing the public key and the other information in a database within the secure environment. The devices manufactured according to the present

application may be reliably and uniquely identified without the need of a digital certificate, unlike the *Fischer* and *Schneier* references.

In general, neither *Fischer* nor *Schneier* teach or suggest the method of manufacturing devices that generate digital signatures as described in claim 26 of the present application. Specifically, neither *Fischer* nor *Schneier* teach or suggest manufacturing a digital signature device within a "secure environment." The references also do not teach or suggest a method for manufacturing devices in a secure environment that generate digital signatures such that each device may be reliably and uniquely identified without the need of a digital certificate.

Given that the combination *Fischer* and *Schneier* clearly does not teach or suggest all elements of any of Appellants' claimed inventions, it is respectfully submitted that the Examiner has failed to establish a *prima facie* case of obviousness with respect to any of claims 22–24 and 27–28. Thus, the combination of *Fischer* and *Schneier* is insufficient to support a rejection under 35 U.S.C. §103(a).

d. Conclusion

It is respectfully submitted that the Examiner has failed to make a *prima facie* case of obviousness. First, there is no motivation to combine the references. Second, there is no reasonable expectation of success in combining the references. And third, the combination of *Fischer* and *Schneier* fails to teach and enable every element of Appellants' claimed inventions as set forth in claim 26. Furthermore, under the doctrine of *In re Fine*, claim 26 should be allowable since claim 1 is nonobvious under 35 U.S.C. §103(a). Therefore, the rejection under §103(a) with respect to the combination of *Fischer* and *Schneier* is improper and should be withdrawn.

2. Appellants' Invention is Not Obvious over the Combination of *Fischer* and *Schneier* Under the *Graham v. John Deere Factors*

For the reasons articulated below, it is respectfully submitted that Appellants' claimed inventions as recited in claim 26 is not obvious over *Fischer* in view of *Schneier*.

a. Scope and content of the prior art

As stated above, *Fischer* describes a CADS system that use certificates via a certificate authority to authenticate digitally signed messages. *Schneier* describes the use of certificates to authenticate a user's public key.

Neither *Fischer* nor *Schneier* is directed to a method of manufacturing devices in a secure environment that generate digital signatures such that each device may be reliably and uniquely identified without the need of a digital certificate. Neither *Fischer* nor *Schneier* is directed to creating the public-private key pair within the secure environment. Neither *Fischer* nor *Schneier* is directed to storing the private key within the device and securely linking the public key with other information by storing the public key and the other information in a database within the secure environment.

b. Differences between the prior art and the claimed invention

Appellants' invention, as recited in claim 26 is directed to a method of manufacturing devices within a secure environment that generate digital signatures such that each device may be reliably and uniquely identified without the need of digital certificates. A public-private key pair is created within the secure environment. The private key, which is stored in the device, is utilized in generating the digital signature for an electronic message. The public key is exportable for use by third parties for authenticating the electronic message and securely linked with other information by storing the public key and the other information in a database within the secure environment. The "other information" involves the information needed to assist the recipient of an electronic message to reliably and uniquely identify the device.

In general, neither of the references, alone or in combination, teach or suggest the method of manufacturing devices within a secure environment that generate digital signatures as set forth in claim 26. In particular, with respect to claim 1 from which claim 26 ultimately depends, the combination of *Fischer* and *Schneier* fails to teach or suggest a method for manufacturing devices that generate digital signatures. The combination of the references fails to teach or suggest manufacturing the devices in a secure environment. The combination of the references fails to teach or suggest that each device may be reliably and

uniquely identified by any means other than a certificate. And finally, the combination of the references fails to teach or suggest a database within a secure environment in which the public key and other information is stored.

c. Level of ordinary skill in the art

Appellants respectfully submit that the level or ordinary skill in the art is one who is skilled in electronic communications and digital signatures.

d. Obviousness analysis

Appellants respectfully submit that the claimed inventions as summarized above would not be obvious to one skilled in electronic communications and digital signatures in view of *Fischer* and *Schneier*. As stated above, neither *Fischer* nor *Schneier* teach or suggest the method of manufacturing devices that generate digital signatures as described in claim 26 of the present application. Specifically, neither *Fischer* nor *Schneier* teach or suggest manufacturing a digital signature device within a "secure environment." The references also do not teach or suggest a method for manufacturing devices that generate digital signatures such that each device may be reliably and uniquely identified without the need of a digital certificate, the devices being manufactured within a secure environment. Since these (and other) aspects of Appellants' inventions are not taught or suggested by any of the references, it is not likely that one of skill in the art would find it obvious to manufacture devices that generate digital signatures according to claim 26 of Appellants' claimed inventions. The omitted elements are not mere variations of the prior art, nor are they so well known that no reference is needed to supply the missing element. Thus, Appellants' claimed invention would not be obvious to one of ordinary skill in the art over *Fischer* and *Schneier*.

e. Conclusion

Appellants respectfully submit that using the *John Deere* factual inquires, the differences between the prior art and the inventions as claimed in claim 26 of the present application would not be obvious to one of ordinary skill in the art. According, Appellants respectfully request withdrawal of the rejection of claim 26 under 35 U.S.C. §103(a).

G. THE PATENT EXAMINER IMPROPERLY REJECTED CLAIMS 29–31 UNDER 35 U.S.C. §103(a) AS BEING OBVIOUS OVER *FISCHER* IN VIEW OF *MENEZES*

In the Office Action dated February 21, 2006, the Examiner rejected claims 29–31 under 35 U.S.C. §103(a) as being allegedly obvious over *Fischer* in view of *Menezes* (Alfred J. Menezes, Handbook of Applied Cryptography 25–31, 546–548, 572–577 (CRC Press 1997)). This rejection is respectfully traversed.

1. The Patent Examiner Failed to Make a Prima Facie Case of Obviousness to Support a Rejection of Claims 29–31 under 35 U.S.C. §103(a) over *Fischer* in View of *MENEZES*

For the reasons articulated below, it is respectfully submitted that the Examiner failed to make a *prima facie* case to support a rejection of any claims under 35 U.S.C. §103(a) over *Fischer* in view of *Menezes*.

a. There is no suggestion or motivation to modify the references or combine the *Fischer* and *Menezes* references

Appellants submit that the Examiner has failed to identify any suggestion or motivation to modify the references or combine the teachings of *Fischer* and *Menezes*. As such, the Examiner has failed to make a *prima facie* case of obviousness under 35 U.S.C. §103(a). Therefore, the rejection is improper and should be withdrawn.

In the Office Action dated February 21, 2006, the Examiner asserted that, as per claim 29, Appellants describe the method of claim 1 which is met by *Fischer*, and the following limitations are met by *Menezes*: authenticating the message of the electronic communication ("EC") using the public key associated with the account in the database identified by the account identifier, and upon successful authentication thereof (*Menezes*: pages 25–26), and sending an EC to each of the third-parties, each EC including the new public key and the third-party account identifier for the respective third-party maintained in the database and associated with the account identified by the account identifier (*Menezes*: page 576). The Examiner combined the teachings of *Fischer* with the teachings of *Menezes* to support a rejection under 35 U.S.C. §103(a). The Examiner indicated that *Menezes* discloses use of public key cryptography in which a message is authenticated using an associated public key and use of a certificate directory in which certificates of users are maintained in a

database. The Examiner also indicated that an EC, which may include a certificate, may be sent to each of the third-parties upon certificate creation or periodically.

Note in particular, again, the Examiner is relying on a certificate authority–based reference, which is a different technical model and actually teaches away from the claimed invention of the present application.

Appellants agree that on pages 25–26, *Menezes* does describe use of public key cryptography in which a message is authenticated using an associated public key. However, like the *Fischer* reference discussed in detail above, on page 576 *Menezes* teaches use of certificates for authenticating information. As explained above, the use of certificates, as described by *Menezes*, is known in the art, and is a factually and technically different model for authentication using public key/private key encryption.

Unlike *Menezes*, which teaches a use of certificates for authentication, the present invention relates to a method of manufacturing devices in a secure environment that generate digital signatures such that each device may be reliably and uniquely identified without the need of a certificate. Furthermore, as discussed in detail above, *Fischer*, which teaches a CADS system, does not describe all the limitations of claim 1 as asserted by the Examiner on page 9 of the February 21, 2006 Office Action. Neither *Fischer* nor *Menezes* teach or disclose systems or methods of manufacturing devices that generate digital signatures such that each device may be reliably and uniquely identified without the need of a digital certificate. Neither reference teaches anything about the manufacturing process for a digital signature device. Therefore, it is factually and legally improper for the Examiner to base a rejection of any claims of the present application on references that describe systems that are so conceptually different from, and teach away from, the present invention.

Given that there is no motivation to modify the teachings of *Fischer* with the teachings of *Menezes*, the Examiner has failed to make a *prima facie* case of obviousness under 35 U.S.C. §103(a) with respect to the combination of *Fischer* and *Menezes*. Therefore, the rejection under 35 U.S.C. §103(a) is improper and should be withdrawn.

Appellants would also like to point out that claims 29–31 depend on claim 1. In other words, claims 29–31 add further limitations to that which is claimed in claim 1. Under

the doctrine of *In re Fine*, 837 F.2d 1071, 5 U.S.P.Q.2d 1596 (Fed. Cir. 1988), if an independent claim is nonobvious under 35 U.S.C. §103(a), then any claim depending there from is nonobvious. Accordingly, since claim 1 is nonobvious, it follows that claims 29–31 are also nonobvious.

b. There is no reasonable expectation of success in combining the *Fischer* and *Menezes* references

Appellants submit that the Examiner has failed to identify a reasonable expectation of success in combining the teachings of *Fischer* and *Menezes*. As such, the Examiner has not established a *prima facie* case of obviousness under 35 U.S.C. §103(a). Therefore, the rejection is improper and should be withdrawn.

In this instance, Appellants submit that there is no reasonable expectation of success in combining the teachings of *Fischer* and *Menezes*, both of which are certificate-authority based references, to support a rejection under 35 U.S.C. §103(a). As discussed in detail above, there is no motivation to combine the cited references. As such, there is no expectation that combining the references would result in a successful combination. Furthermore, there is no expectation that combining the references would result in Appellants' claimed inventions, as will be discussed in greater detail below.

c. The combination of the *Fischer* and *Menezes* references does not teach or suggest all elements of Appellants' claimed invention

Appellants assert that the combination of *Fischer* and *Menezes* fails to teach or suggest all elements of Appellants' claimed invention, and therefore is insufficient to support a rejection under 35 U.S.C. §103(a).

As explained above, Appellants' inventions are generally directed to methods of manufacturing devices in a secure environment that generate digital signatures such that each device may be reliably and uniquely identified without the need of a digital certificate. The methods claimed in claims 29–31 recite creating a public-private key pair within the secure environment, storing the private key within the device, and securely linking the public key with other information by storing the public key and the other information in a database within the secure environment. The device manufactured according to the claims at issue in

the present application may be reliably and uniquely identified without the need of a digital certificate, unlike the *Fischer* and *Menezes* references.

In general, neither *Fischer* nor *Menezes* teach or suggest the method of manufacturing devices that generate digital signatures as recited in claims 29–31 of the present application. Specifically, neither *Fischer* nor *Menezes* teach or suggest manufacturing a digital signature device within a "secure environment." The references also do not teach or suggest a method for manufacturing devices in a secure environment that generate digital signatures such that each device may be reliably and uniquely identified without the need of a digital certificate.

Given that the combination *Fischer* and *Menezes* clearly does not teach or suggest all elements of any of Appellants' claimed inventions, it is respectfully submitted that the Examiner has failed to establish a *prima facie* case of obviousness with respect to any of claims 29–31. Thus, the combination of *Fischer* and *Menezes* is insufficient to support a rejection under 35 U.S.C. §103(a).

d. Conclusion

It is respectfully submitted that the Examiner has failed to make a *prima facie* case of obviousness. First, there is no motivation to combine the references. Second, there is no reasonable expectation of success in combining the references. And third, the combination of *Fischer* and *Menezes* fails to teach and enable every element of Appellants' claimed inventions as set forth in claims 29–31. Furthermore, under the doctrine of *In re Fine*, claims 29–31 should be allowable since claim 1 is nonobvious under 35 U.S.C. §103(a). Therefore, the rejection under §103(a) with respect to the combination of *Fischer* and *Menezes* is improper and should be withdrawn.

2. Appellants' Invention is Not Obvious over the Combination of *Fischer* and *Menezes* Under the *Graham v. John Deere Factors*

For the reasons articulated below, it is respectfully submitted that Appellants' claimed inventions as recited in claims 29–31 are not obvious over *Fischer* in view of *Menezes*.

a. Scope and content of the prior art

As stated above, *Fischer* describes a CADS system that use certificates via a certificate authority to authenticate digitally signed messages. *Menezes* also describes the use of certificates for authentication.

Neither *Fischer* nor *Menezes* is directed to a method of manufacturing devices in a secure environment that generate digital signatures such that each device may be reliably and uniquely identified without the need of a digital certificate. Neither *Fischer* nor *Menezes* is directed to creating the public/private key pair within the secure environment. Neither *Fischer* nor *Menezes* is directed to storing the private key within the device and securely linking the public key with other information by storing the public key and the other information in a database within the secure environment.

b. Differences between the prior art and the claimed invention

Appellants' invention, as recited in claims 29–31 are directed to a method of manufacturing devices within a secure environment that generate digital signatures such that each device may be reliably and uniquely identified without the need of digital certificates. A public-private key pair is created within the secure environment. The private key, which is stored in the device, is utilized in generating the digital signature for an electronic message. The public key is exportable for use by third parties for authenticating the electronic message and securely linked with other information by storing the public key and the other information in a database within the secure environment. The "other information" involves the information needed to assist the recipient of an electronic message to reliably and uniquely identify the device.

In general, neither of the references, alone or in combination, teach or suggest the method of manufacturing devices within a secure environment that generate digital signatures as set forth in claims 29–31. In particular, with respect to claim 1 from which claims 29–31 ultimately depend, the combination of *Fischer* and *Menezes* fails to teach or suggest a method for manufacturing devices that generate digital signatures. The combination of the references fails to teach or suggest manufacturing the devices in a secure environment. The combination of the references fails to teach or suggest that each device

may be reliably and uniquely identified by any means other than a certificate. And finally, the combination of the references fails to teach or suggest a database within a secure environment in which the public key and other information is stored.

With respect to claim 29 which builds upon the elements presented in claim 1, the combination of *Fischer* and *Menezes* fails to teach or suggest, *inter alia*, receiving an electronic communication ("EC"), authenticating the message of the EC using the original public key associated with the account in the database identified by the account identifier, and sending an EC to each of the third-parties. The Examiner contended that this element was found in the *Fischer* reference at column 2, lines 19–37. However, as already discussed, *Fischer* describes the use of digital certificates for authenticating digital signatures. This is in stark contrast to the present application in which no digital certificates are used.

With respect to claim 30 which builds upon the elements presented in claims 1 and 29, the combination of *Fischer* and *Menezes* fails to teach or suggest, *inter alia*, the step of digitally signing a message involving a new public key of the user and a third-party account identifier.

Likewise, with respect to claim 31 which builds upon the elements presented in claims 1 and 29, the combination of *Fischer* and *Menezes* fails to teach or suggest, *inter alia*, the step of sending the EC received from the user to each of the third-parties.

c. Level of ordinary skill in the art

Appellants respectfully submit that the level or ordinary skill in the art is one who is skilled in electronic communications and digital signatures.

d. Obviousness analysis

Appellants respectfully submit that the claimed inventions as summarized above would not be obvious to one skilled in electronic communications and digital signatures in view of *Fischer* and *Menezes*. As stated above, neither *Fischer* nor *Menezes* teach or suggest the method of manufacturing devices that generate digital signatures as recited in claims 29–31 of the present application. Specifically, neither *Fischer* nor *Menezes* teach or suggest manufacturing a digital signature device within a "secure environment." The references also do not teach or suggest a method for manufacturing devices that generate digital signatures

such that each device may be reliably and uniquely identified without the need of a digital certificate, the devices being manufactured within a secure environment. Since these (and other) aspects of Appellants' inventions are not taught or suggested by any of the references, it is not likely that one of skill in the art would find it obvious to manufacture devices that generate digital signatures according to claims 29–31 of Appellants' claimed inventions. The omitted elements are not mere variations of the prior art, nor are they so well known that no reference is needed to supply the missing element. Thus, Appellants' claimed invention would not be obvious to one of ordinary skill in the art over *Fischer* and *Menezes*.

e. Conclusion

Appellants respectfully submit that using the *John Deere* factual inquires, the differences between the prior art and the inventions as claimed in claims 29–31 of the present application would not be obvious to one of ordinary skill in the art. According, Appellants respectfully request withdrawal of the rejection of claims 29–31 under 35 U.S.C. §103(a).

H. SUMMARY OF THE ARGUMENT

As described above, the Examiner rejected pending claims 1–5 and 21–31 in a final rejection mailed February 21, 2006. Those claims are the subject of this appeal. For the reasons discussed in detail above, the Appellants' submit that the Board should overrule the Examiner's rejections of the claims.

Specifically, in regards to the Examiner's rejection of claims 1–5 and 21–31 under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claim 17 of U.S. Patent No. 6,915,430, over claim 18 of U.S. Patent No. 6,892,302, over claim 28 of copending U.S. Patent Application No. 10/248,626, and over claim 35 of copending U.S. Patent Application No. 10/248,629, Appellants remain willing to submit a terminal disclaimer directed to U.S. Patent No. 6,915,430, U.S. Patent No. 6,892,302, and U.S. Patent Application No. 10/248,626 because of the similarity in subject matter claimed in each of these references. However, Appellants do not agree with and hereby continue to traverse the Patent Examiner's assertion that the claims of the present application are not

patentably distinct from the claims of U.S. Patent Application No. 10/248,629 (now U.S. Patent No. 6,959,381) ("the '381 Patent") because there is no disclosure, teaching, or suggestion in the '381 Patent supporting the rejection of claims 1–5 and 21–31 under the judicially created doctrine of obviousness-type double patenting.

Furthermore, the amendment filed on August 18, 2006 pursuant to 37 C.F.R. §1.116 addressed the Examiner's rejections under 35 U.S.C. §112. Appellants respectfully request the entry of this amendment and withdrawal of these rejections.

Finally, none of the references cited by the Examiner, either singularly or in combination, teach, suggest, or describe the invention of the present application. There is no disclosure, teaching, or suggesting in the *Fischer*, *Spies*, *Ramasubramani*, *Schneier*, or *Menezes* references that would anticipate or make the claims of the present invention obvious. Because these references do not disclose, teach, or suggest, singularly or in combination, all of the elements specified in the claims of the present application, the record of this case indicates by a preponderance of the evidence that the claims of the present application should be patentable over the cited art. None of the claims or disclosures of these references make obvious or suggest a method of manufacturing devices within a secure environment that generate digital signatures such that each device may be identified by creating a public-private key pair, storing the private key within the device, and securely linking the public key with other information by storing the public key and the other information in a database within the secure environment.

For at least the reasons stated above, Appellants respectfully request that the Board of Patent Appeals and Interferences reverse the Examiner's rejections of the claims of the present invention and allow claims 1–5 and 21–31.

VIII. CLAIMS APPENDIX

1. (Previously Presented) A method of manufacturing devices that generate digital signatures such that each device may be reliably and uniquely identified, the devices being manufactured within a secure environment, comprising the steps of:
   a. creating a public-private key pair within the secure environment, the private key for utilization in generating a digital signature for an electronic message, the public key exportable for use by third parties in connection with authenticating the electronic message;
   b. storing the private key within the device against the possibility of divulgement thereof by the device; and
   c. securely linking the public key with other information by storing the public key and the other information in a database within the secure environment.

2. (Original) The method of claim 1, wherein each private-public key pair is created within each device based on a random number produced by a random number generator disposed within each device.

3. (Original) The method of claim 2, wherein each digital signature generated by each device is a random number.

4. (Previously Presented) The method of claim 1, wherein the other information comprises respective security features and a manufacturing history of each device.

5. (Previously Presented) The method of claim 1, further comprising the step of identifying a particular manufactured device by authenticating a message using one of a plurality of public keys in the database within the secure environment, a digital signature for the message having been generated by the particular manufactured device.

6. — 20. (Cancelled)

21. (Previously Presented) The method of claim 1, wherein the public key and information linked therewith is obtained from a Secure Entity.

22. (Previously Presented) The method of claim 1, wherein the public key and the other information stored in the database includes the identity of a plurality of third-parties with which an account is maintained, the accounts being identified by one of a plurality of third-party account identifiers.

23. (Previously Presented) The method of claim 22, wherein the public key and the other information of the users is indexed in the database by unique account identifiers such that the public key and the other information for a user is retrievable from the database based on the account identifier.

24. (Previously Presented) The method of claim 23, wherein the public key is the unique account identifier.

25. (Previously Presented) The method of claim 1, wherein the public key and the other information stored in the database for each user further includes user-specific information.

26. (Previously Presented) The method of claim 25, wherein the user-specific information includes the name and address of the user.

27. (Previously Presented) The method of claim 1, further comprising the step of establishing an account on behalf of a user of a device with a third-party by communicating the public key of the device and the other information linked with the public key from the database to the third-party.

28. (Previously Presented) The method of claim 1, wherein the public key of the device and the other information linked with the public key is communicated to a third party upon the request of the third-party.

29. (Previously Presented) The method of claim 1, wherein the public key is an original public key and further comprising the step of updating the original public key and other information of a user maintained with at least two independent third-parties with a new public key of the user, comprising the steps of:
    a. receiving an EC, the EC including an account identifier and a message including the new public key and a digital signature therefore,
    b. authenticating the message of the EC using the original public key associated with the account in the database identified by the account identifier, and upon successful authentication thereof,
    c. sending an EC to each of the third-parties, each EC including the new public key and the third-party account identifier for the respective third-party maintained in the database and associated with the account identified by the account identifier.

30. (Previously Presented) The method of claim 29, further comprising the step of digitally signing a message involving the new public key of the user and a third-party account identifier.

31. (Previously Presented) The method of claim 29, further comprising the step of sending the EC received from the user to each of the third-parties.

IX. EVIDENCE APPENDIX

A. Appellants' Amendment under 37 C.F.R. §1.116 filed August 18, 2006.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventors:	Wheeler, et al.	**Examiner:**	Kevin R. Schubert
		Group Art Unit:	2137
Application No.	09/923,213	**Docket No.:**	10399-34384
Filed:	August 6, 2001	**Confirmation No.:**	8986
Title:	MANUFACTURING UNIQUE DEVICES THAT GENERATE DIGITAL SIGNATURES		

CERTIFICATE UNDER 37 CFR 1.8: I hereby certify that this correspondence is being □ deposited with the United States Postal Service as First Class mail in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450, or □ filed via facsimile at 571 272 8300 or ☒ filed via EFS-Web, on August 18, 2006.

By: _____
John R. Harris

AMENDMENT UNDER 37 C.F.R. § 1.116

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Sir:

Responsive to the Office Action dated February 21, 2006, please amend the form the claims of the above-referenced application as follows and consider the appended remarks. Note that this Amendment is being submitted prior to filing of an appeal brief in this case, for the purpose of removing certain alleged indefiniteness issues in claim wording from the appeal.

This amendment is submitted in compliance 37 C.F.R. § 1.116 and contains the following separate sections that start on a separate sheet:

The **Listing of Claims** begins on page 2 of this paper.

Remarks begin on page 5 of this paper.

LISTING OF CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method of manufacturing devices that generate digital signatures such that each device may be reliably and uniquely identified, the devices being manufactured within a secure environment, comprising the steps of:
   a. creating a public-private key pair within the secure environment, the private key for utilization in generating a digital signature for an electronic message, the public key exportable for use by third parties in connection with authenticating the electronic message;
   b. storing the private key within the device against the possibility of divulgement thereof by the device; and
   c. securely linking the public key with other information by storing the public key ~~in association with~~ and the other information in a database within the secure environment.

2. (Original) The method of claim 1, wherein each private-public key pair is created within each device based on a random number produced by a random number generator disposed within each device.

3. (Original) The method of claim 2, wherein each digital signature generated by each device is a random number.

4. (Previously Presented) The method of claim 1, wherein the other information comprises respective security features and a manufacturing history of each device.

5. (Previously Presented) The method of claim 1, further comprising the step of identifying a particular manufactured device by authenticating a message using one of

a plurality of public keys in the database within the secure environment, a digital signature for the message having been generated by the particular manufactured device.

6. — 20. (Cancelled)

21. (Previously Presented) The method of claim 1, wherein the public key and information linked therewith is obtained from a Secure Entity.

22. (Currently Amended) The method of claim 1, wherein the ~~PuK-linked~~ other information stored in the database includes the identity of a plurality of third-parties with which an account is maintained, the accounts being identified by one of a plurality of third-party account identifiers.

23. (Currently Amended) The method of claim 22, wherein the ~~PuK-linked account~~ public key and the other information ~~of the users~~ is indexed in the database by unique account identifiers such that the ~~PuK-linked account~~ public key and the other information for a user is retrievable from the database based on the account identifier.

24. (Currently Amended) The method of claim ~~22~~ 23, wherein the public key is the unique account identifier.

25. (Currently Amended) The method of claim 1, wherein the ~~PuK-linked~~ public key and the other information ~~maintained~~ stored in the database for each user further includes user-specific information.

26. (Currently Amended) The method of claim ~~12~~ 25, wherein the user-specific information includes the name and address of the user.

27. (Currently Amended) The method of claim ~~6~~ 1, further comprising the step of establishing an account on behalf of a user of a device with a third-party by communicating the public key of the device and the other information linked with the public key from the database to the third-party.

28. (Currently Amended) The method of claim ~~27~~ 1, wherein the public key of the device and the other information linked with the public key is communicated to a third party upon the request of the third-party.

29. (Currently Amended) The method of claim 1, wherein the public key is an original public key and further comprising the step of updating the ~~PuK-linked accounts~~ original public key of a user maintained with at least two independent third-parties with a new public key of the user, comprising the steps of:
    a. receiving an EC, the EC including an account identifier and a message including the new public key and a digital signature therefor,
    b. authenticating the message of the EC using the original public key associated with the account in the database identified by the account identifier, and upon successful authentication thereof,
    c. sending an EC to each of the third-parties, each EC including the new public key and the third-party account identifier for the respective third-party maintained in the database and associated with the account identified by the account identifier.

30. (Previously Presented) The method of claim 29, further comprising the step of digitally signing a message involving the new public key of the user and a third-party account identifier.

31. (Previously Presented) The method of claim 29, further comprising the step of sending the EC received from the user to each of the third-parties.

REMARKS

Claims 1–5 and 21–31 are pending in this application. In a final rejection mailed February 21, 2006, the examiner made the following rejections:

- Claims 1–5 and 21–31 were rejected on grounds of nonstatutory double patenting over U.S. Patent Nos. 6,915,430 and 6,892,302 and copending U.S. Patent Application Nos. 10/248,626 and 10/248,629;
- Claims 1 and 24–29 were rejected under 35 U.S.C. § 112, second paragraph;
- Claims 1, 4–5, 21, and 25 were rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,422,953 issued to *Fischer*;
- Claims 2–3 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Fischer* in view of U.S. Patent No. 6,230,269 issued to *Spies, et al.*;
- Claims 22–24 and 27–28 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Fischer* in view of U.S. Patent No. 6,233,577 issued to *Ramasubramani et al.*;
- Claim 26 was rejected under 35 U.S.C. § 103(a) as being unpatentable over *Fischer* in view of *Schneier*; and
- Claims 29–31 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Fischer* in view of *Menezes*.

The Applicants submitted a Notice of Appeal and a Pre-Appeal Brief Request for Review on May 22, 2006. The Panel responded on June 13, 2006 to the Applicants' Pre-Appeal Brief Request for Review maintaining the rejections of claims 1–5 and 21–31 and stating that the application remains under appeal. The Applicants plan to file an Appeal Brief for

submission to the Board of Patent Appeals and Interferences ("BPAI") on or before August 21, 2006.

The present amendment is submitted under Rule 116 in response to the Examiner's rejections under 35 U.S.C. § 112, second paragraph in order to remove these issues from the appeal. The Applicants will address the Examiner's remaining rejections in the Appeal Brief. The Applicants submit that the current amendments go to the form of the claims and do not affect the substantive merits of the application.

It is believed that the entry of this Amendment will place the claims in better form for consideration on appeal and raise no new issues not previously considered by the examiner. Entry of this Amendment and reconsideration of the 35 U.S.C. § 112 rejections is therefore respectfully requested. If the Examiner believes that a telephone conference with the Applicant's attorneys would be advantageous to the disposition of this case then the Examiner is encouraged to telephone the undersigned at 404 504 7720.

Respectfully submitted,

MORRIS, MANNING & MARTIN, LLP

John R. Harris
Reg. No. 30,388

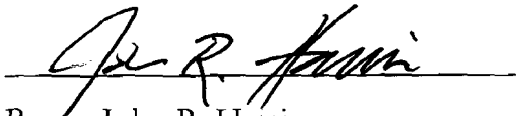
MORRIS, MANNING & MARTIN, LLP
1600 Atlanta Financial Center
3343 Peachtree Road, NE
Atlanta, GA 30326
(404) 233-7000
(404) 365-9532 - fax
jrh@mmmlaw.com
Dated: August 18, 2006

Docket No. 10399-34384

X. RELATED PROCEEDINGS APPENDIX

None.

Respectfully submitted,



By: John R. Harris
Reg. No. 30,388

By: Heather Champion Brady
Reg. No. 54,023

MORRIS, MANNING & MARTIN, LLP
3343 Peachtree Road, N.E.
1600 Atlanta Financial Center
Atlanta, Georgia 30326
(404) 233-7000
Email: jrh@mmmlaw.com
Docket: 10399–34384